U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

May 12, 2022

BY ECF, E-MAIL, and HAND

The Honorable John G. Koeltl
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

Re: *United States v. Arthur Hayes*, 20 Cr. 500 (JGK)

Dear Judge Koeltl:

The Government respectfully submits this letter in advance of the sentencing of defendant Arthur Hayes, currently scheduled for May 20, 2022 at 2 p.m., and in response to the defendant's sentencing memorandum ("Def. Mem").

Arthur Hayes is the CEO, co-founder, and 30 percent owner of BitMEX, an incredibly successful cryptocurrency company, which he designed to operate in violation of the Bank Secrecy Act ("BSA"), the U.S. law designed to prevent money laundering and to assist the tracking of proceeds of criminal activity. Hayes profited greatly from BitMEX, personally earning over one hundred million dollars, while willfully and continuously operating the Company in violation of the BSA, by failing to implement an anti-money laundering ("AML") program. During the charged period, as BitMEX grew to become one of the largest cryptocurrency derivatives platforms in the world, the defendant enabled BitMEX to allow its users to transact trillions of dollars anonymously, because he decided not to implement a know-your-customer ("KYC") procedure. The defendant prominently advertised BitMEX's lack of KYC and AML, through its website, blogposts that he authored, and in the media. The lack of KYC and AML drew precisely the bad actors which the BSA intends to deter, but when the defendant learned about suspicious transactions on BitMEX's platform, he caused the Company to fail to file suspicious activity reports ("SARs") with the Department of Treasury. To maintain the fiction that BitMEX was outside of the scope of the BSA, the defendant lied repeatedly and exhibited deep disrespect for the law, including the BSA and U.S. commodities laws.

The proper sentence in this case should reflect his history and characteristics, including the talent and sophistication which he used to create a cryptocurrency platform designed to operate outside the law; the seriousness of this offense; the need to promote respect for the law which he willfully violated; to afford proper deterrence, both specific and general, in this important case that an entire industry is observing closely; and the requirement to avoid sentencing disparities among defendants who commit similar misconduct. For these and the reasons set forth in greater detail

below, a significant sentence of incarceration, above the applicable Sentencing Guidelines range of 6 to 12 months, is necessary to comply with the purposes set forth in 18 U.S.C. § 3553(a).

I. Hayes' Conduct

A. Background of BitMEX

Hayes, Ben Delo, and Sam Reed are the co-founders and equal owners of BitMEX. They launched BitMEX in 2014. (Presentence Investigation Report ("PSR") ¶ 14). During applicable periods from that launch to at least in or about October 2020, the Company offered financial derivatives, including futures contracts and swaps, tied to the price of Bitcoin and other cryptocurrencies, which settled in Bitcoin. (PSR ¶¶ 14–15). Because BitMEX operated in the United States, including through offering its products to U.S. customers and operating offices in the United States, the Company was a futures commission merchant ("FCM"), which is required under the Commodity Exchange Act ("CEA") to register with the Commodity Futures Trading Commission ("CFTC"), and is a financial institution which must comply with the Bank Secrecy Act. (PSR ¶ 15). From its launch in 2014, BitMEX acted in violation of the BSA; Hayes and his co-conspirators began willfully violating that law by at least in or about September 2015, when the CFTC issued regulatory orders announcing its view that cryptocurrency is a commodity, and the defendants knew their failure to implement an AML program while operating in the United States was unlawful.

As CEO, Hayes was a leader in BitMEX's criminal failure to comply with the BSA. (PSR ¶¶ 19, 56). He was a critical organizer of the ongoing decisions not to implement an AML program at BitMEX, while operating in the United States. (PSR ¶ 56). When Hayes helped launch BitMEX, he had over half a decade experience in financial services, and thus fostered BitMEX's lack of compliance functions. (PSR ¶¶ 56, 98).

Beginning with BitMEX's launch, Hayes was consistently focused on avoiding KYC requirements. In its earliest days, BitMEX advertised that it did not perform know-your-customer checks. Shortly before the launch of the program for live trading in November 2014, Hayes wrote to Delo that BitMEX would not do any KYC, saying "Basically just valid email address until we feel significant pressure to do otherwise." In about 2015, the website advertised that "No real name or other advanced verification is required on BitMEX." (PSR ¶ 18). In a February 2017 blog post, Hayes wrote that "KYC and AML violations are used by governments worldwide to harass companies." https://blog.bitmex.com/lockdown/ (accessed May 12, 2022). Until at least August 2017, BitMEX's registration page required users to provide a username, email address, and password; but explicitly stated that first and last name were "not required" to register and were only "used for verification purposes if you lose your two-factor auth[entication]" for account login. While that language on BitMEX's website was later removed, BitMEX still did not require users to verify their identities until after the Indictment was unsealed.

B. Hayes Closely Followed, and Defied, U.S. Law

Hayes and his co-defendants followed global regulation of cryptocurrency, particularly from the United States, very closely. Those regulations guided their business decisions. First, the

defendants chose to incorporate in the Seychelles specifically because the country "had no clarity on Bitcoin." (PSR ¶ 16). Second, the defendants designed the very architecture of BitMEX to avoid KYC regulations, stating that they chose to transact with BitMEX's customers exclusively in Bitcoin because, as of 2014, their view was that there was no "gov[ernmen]t regulation covering KYC or AML" for such transactions. (PSR ¶ 16).[1]

Hayes and his co-founders soon came to understand that the decision to only accept Bitcoin did not exempt them from KYC and AML regulations. In September 2015, the CFTC issued two public administrative actions, which announced the Commission's view that cryptocurrency was a commodity subject to regulation under the CEA. (PSR ¶ 17(b)). As Hayes acknowledges in his sentencing submission, he "reviewed these orders and concluded that, under the CFTC's new approach to regulation of cryptocurrency, BitMEX could be subject to CFTC jurisdiction, including a requirement to conduct KYC, if the company served U.S. customers." Def. Mem. at 11.

Given the choice between complying with the BSA or withdrawing from the United States, the defendants putatively chose the latter: they put a notice on BitMEX's website and in its terms of service stating that U.S. customers were forbidden from creating accounts, and restricted individuals from creating an account using an internet protocol ("IP") address from the United States. (PSR ¶ 17).[2] However, these controls were a sham. Hayes knew that the controls were easily evaded, and did not take simple steps to restrict more U.S. customers from accessing the platform.

Hayes knew U.S. customers continued to access BitMEX through several means. First, BitMEX already had a significant number of U.S. users in September 2015 and made no effort to remove them. (PSR ¶ 24). Second, he and his co-defendants did not actually bar U.S. IP addresses from the platform. Instead, BitMEX only ran a single IP address check when new users created accounts, even though Hayes knew that users could easily avoid the initial check, including by using virtual private network services ("VPN")[3] and then make subsequent logins from U.S. IP addresses. (PSR ¶¶ 29–32). Third, Hayes intentionally marketed to U.S. customers, including through his appearances on U.S. media outlets and through the BitMEX affiliate user program.

---

[1] The Department of Treasury had in 2013 published public guidance documents that it interpreted the BSA as covering institutions that exchanged between cryptocurrency and fiat currency.

[2] Even these restrictions did not mean the Company was not operating in the United States, since Reed, and later Greg Dwyer, were physically based in the United States while carrying out their duties, and BitMEX had numerous other employees physically present in the U.S., including from an office in Manhattan.

[3] The defendant suggests that he did not believe "it w[as] technologically possible to block customers using a VPN from gaining access to the BitMEX platform." Def. Mem. at 13 n.7. By the time BitMEX began putatively blocking U.S. users, however, other companies had done so for years. *See, e.g.*, Netflix restricts streaming from abroad, available at https://money.cnn.com/2015/01/05/technology/netflix-vpn (describing Netflix corporate statement that "Virtually crossing borders to use Netflix is a violation of our terms of use because of content licensing restrictions, and we employ standard measures to prevent this kind of use.").

(PSR ¶¶ 33–35). Fourth, the defendant allowed some prominent users who he personally knew were U.S. persons to access and trade on BitMEX's platform openly.[4] (PSR ¶¶ 17, 24–27). Finally, as Hayes acknowledges, users whose accounts were closed because they had been flagged as from the United States could still open a new account, even if they used the exact same email address as the closed account. Def. Mem. at 14 n.9. The Government has identified multiple such users who did precisely that and then continued to freely operate on BitMEX.

The presence of U.S. users was far from incidental. On the contrary, as late as July 2017, nearly two years after claiming to have banned U.S. users, Hayes received a report from Greg Dwyer, a BitMEX employee, that showed that the "United States remains the most popular country by visits and average number of active users per day." (PSR ¶ 21).[5] Subsequent monthly revenue reports continued to show the presence of U.S. users on BitMEX. (PSR ¶ 22). Hayes claims that BitMEX turned away large numbers of U.S. users. Deft. Mem. at 14. His primary source for that claim is the pretrial report of a defense "expert" witness, but as the Government's briefing demonstrated, that report was riddled with errors. Dkt. No. 280 at 15–17, 18–21. Hayes also acknowledges that when BitMEX did shut down U.S. accounts, the same user could easily create a new account, using the same email address, a practice that appears to have been common. In fact, Hayes well knew that there were no effective controls and that large numbers of U.S. users freely traded on the platform.

Despite Hayes and his co-founders' knowledge that allowing these users meant that BitMEX was subject to U.S. law including the BSA, BitMEX never required all users to provide their real names and identification documents until after the unsealing of the Indictment; nor did the Company file any SARs with FinCEN between its launch and the unsealing of the Indictment, despite ample knowledge of suspicious activities.

C. The Defendant Knew that BitMEX was a Tool for Criminal Activity

As a result of Hayes' decisions not to implement an AML program, BitMEX became a tool for money laundering and criminal activity, which Hayes knew and did little to stop. Because BitMEX did not require KYC, (PSR ¶¶ 20, 26), the full scope of criminal conduct on BitMEX will never be known. BitMEX, still owned by Hayes, Delo, and Reed, accepted a settlement with the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") in which it neither

---

[4] Hayes describes this user's continued access to BitMEX as "some sort of internal breakdown in BitMEX's process," Def. Mem. at 15 n.10, but the evidence, including that described in the PSR, shows that was an intentional decision by BitMEX's management so as not to "make enemies." (PSR ¶ 25).

[5] These reports belie Hayes' claim that the company was focused on Chinese users from the second half of 2015 onward. Def. Mem. at 7-8. Additionally, Hayes' claim that he "inferred" that web traffic showing a user's IP address was in the United States "was actually originating in China" because many Chinese customers used VPNs, Def. Mem. at 13 n.7, is not credible. In the reports that identify the U.S. as the most popular country for BitMEX users in 2017, there is no suggestion that any of these users were actually in China, and those reports separately list China as a country with large numbers of visits and users.

admitted nor denied FinCEN's finding that it had conducted more than $200 million in suspicious transactions, and that the Company had failed to file SARs on nearly 600 specific suspicious transactions. (PSR ¶ 42); FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act, *available at* https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures. The Government has seen BitMEX surface repeatedly in its own criminal investigations, an indication of the consequences of BitMEX's failure to implement any AML controls. For instance, Jeremy Spence, a U.S. citizen prosecuted by this Office, pled guilty to commodities fraud which included his misrepresentations regarding his trading positions on BitMEX. 21 Cr. 116 (LAK) (S.D.N.Y.). Previously convicted felon Michael Patryn, one of the founders of the crypto company QuadrigaCX, now insolvent and possibly fraudulent, had an account on BitMEX. British hacker Elliot Gunton, currently charged by federal authorities in California, also had an account linked to BitMEX.

A representative example occurred in May 2018. On May 4 an attorney in Germany contacted BitMEX's support email address, stating that his client had been hacked and the proceeds may have been laundered through BitMEX. This email was passed to Hayes, along with a message from a BitMEX employee identifying the user ID for the account containing the stolen proceeds. BitMEX froze the account and Hayes instructed the victim's attorney to obtain a Seychelles court order, but after a few weeks, the attorney responded that was a particularly challenging process. The suspicious user began repeatedly emailing BitMEX's support staff to complain about his account freeze. After a few weeks, Hayes told his employee to unfreeze the account, because the victim "has not come back to us yet with a proper court order." The account was unfrozen; the suspicious user could then withdraw what Hayes' own employee had identified as "the stolen bitcoin" from BitMEX's platform, which the user promptly did. (PSR ¶¶ 43–44).[6] Hayes did not report this encounter to law enforcement or thereafter implement an AML program.

The consequences of this action were raised again a few months later, when German police contacted BitMEX's support desk requesting additional information about that same hack incident. BitMEX then filed a report with the Seychelles regulator, but did not include the kind of information required under U.S. law, including the email address which BitMEX employees themselves recognized as involved in the money laundering, nor did they inform the Seychelles regulator that BitMEX had unfrozen the account and allowed the suspected user to withdraw the potential criminal proceeds. (PSR ¶ 44).

BitMEX's deficient compliance program extended to its treatment of U.S. sanctions laws. From the earliest days of the company, compliance consultants offered their services to BitMEX, and mentioned that they offered sanctions programs. BitMEX counterparties also sometimes mentioned the need for a counter-sanctions program. However, Hayes did not take these statements seriously. In about January 2017, Hayes and Delo both told Iranian customers that they were free to trade. (PSR ¶ 45). By no later than October 2017, Hayes knew that the company could not transact with individuals on the U.S. sanctions list, and implemented some controls designed to try to restrict such transactions. (PSR ¶ 45). However, he did not take steps to ensure that the customers

[6] This incident belies Hayes' statement that he did not "condone[] any illegal transaction activity on the platform." Def. Mem. at 16.

he had authorized had been removed from the platform. (PSR ¶ 45). Without an adequate KYC program, BitMEX could never be sure it was not dealing with sanctioned individuals, who could use the same simple methods to evade the controls as those used by U.S. persons. As a result, BitMEX internal reports shared with the defendant showed that BitMEX continued to earn revenue from customers in Iran through at least April 2018, and Delo understood as late as November 2018 that the company did not have "strict enforcement of US sanctions against Iran etc.," and sometimes "let these people slip through the cracks." (PSR ¶ 46).

D. Hayes Repeatedly Lied About BitMEX's Operations

As the public face of BitMEX, Hayes was often asked about whether BitMEX needed to comply with the BSA. He could only maintain BitMEX's claim to be outside of U.S. jurisdiction through a series of lies. For example, in March 2016 when a CFTC letter to a different cryptocurrency platform was released, implying that the platform was in violation of the CEA and BSA by offering its products to people in the United States, Hayes lied to an associate of his that the letter was "Not a problem for us we don't allow US residents." (PSR ¶ 36). A few months later, after the CFTC had taken an administrative action against another cryptocurrency company for operating as an unregistered FCM, Hayes again lied, and said that BitMEX would not be affected because, unlike that company, "BitMEX openly does not server [sic] US customers. They are not allowed to enter the platform. We block all US IP addresses." (PSR ¶ 36).

Hayes similarly lied to a *Wall Street Journal* reporter the following year, stating "Due to CFTC regulations, BitMEX does not service Americans." (PSR ¶ 37). After the CFTC and SEC brought actions against a cryptocurrency platform called 1Broker for various offenses, including violations of the BSA, in September 2018, Hayes sent an email to all employees of BitMEX, falsely asserting that "[t]here are important differences between 1Broker and the business of BitMEX, and I want to remind and reassure you that BitMEX prohibits residents of the US from holding positions or entering into contracts on BitMEX." (PSR ¶ 39).

Hayes also made other misrepresentations to support BitMEX's operations. From in about 2016 through at least 2018, Hayes, Delo, and others at the Company made a series of false statements and submitted false documents to the Hong Kong branch of HSBC regarding Shine Effort, a BitMEX affiliate. Hayes, Delo, and other BitMEX employees told HSBC that Shine Effort was actually independent and owned by Delo, with no connection to cryptocurrency. These false statements were designed to allow BitMEX access to bank accounts for payment of various corporate expenses and make U.S. dollar wire transfers. (PSR ¶ 47). Hayes conspired to make these misrepresentations because of his belief that were HSBC to learn the truth, the bank would decline to allow Shine Effort to open a bank account, or later that HSBC would close the account. For example, in April 2017, HSBC requested additional information about the Shine Effort account. (PSR ¶ 50). Hayes contacted an associate about BitMEX's desire to "open a few other backup accounts for our subsidiary," namely Shine Effort. Hayes wrote "we have a hsbc sub that isn't outwardly associated with bitmex" and "we want an additional bank account / so technically not crypto related". Similarly, in October 2018, when trying to obtain false documents to submit to the bank that omitted references to cryptocurrency, (PSR ¶ 53), Hayes wrote to a BitMEX

employee he was trying to obtain a contract but "we want to make sure it does not mention bitcoin."[7]

E. Hayes Caused BitMEX to Unlawfully Offer Risky Products to Retail Investors

Along with the defendant's violation of the BSA came multiple civil violations of the CEA, the law designed to protect investors and the integrity of the commodities markets. Among those violations was his offering of risky extremely leveraged derivatives to "retail" customers (as opposed to sophisticated investors, called "eligible contract participants" under the CEA, 7 U.S.C. §§ 1a(28)(A)(i)(I)(bb) and (18)). Indeed, the defendant was quite clear that he wanted to appeal to such "retail" customers. https://blog.bitmex.com/bitmex-vs-cme-futures-guide/ (accessed May 12, 2022) (December 2017 blog post in which the defendant compared his interest in "retail" as opposed to "professional investors"); Def. Mem. at 7–8 ("BitMEX was able to offer significantly greater leverage, which was a key selling point for retail investors in China."). But while Hayes sometimes dressed up his interest as ensuring that retail traders had the opportunity to trade the potentially lucrative products, at other times, he was quite plain that he knew that BitMEX's products were dangerous for retail traders. In a presentation still available on YouTube, found at https://www.youtube.com/watch?v=Ljw9ulT2NHE, approximately minute 8:00, Hayes describes that BitMEX only became successful when he realized that "[t]here are people who offer similar types of products but are focusing on degenerate gamblers, a.k.a. retail traders in Bitcoin, so why don't we do the same?" He continued that he decided to create "the world's highest leverage Bitcoin-U.S. dollar product," recognizing that this was the "world's most leveraged product to trade Bitcoin/U.S. dollars" "on the most volatile asset in the history of the world." BitMEX's support staff was often flooded with emails from users who had lost thousands of dollars, or even said they were contemplating suicide, after the user lost large sums on BitMEX's platform.

F. Hayes Mischaracterizes BitMEX's Remedial Efforts

In his sentencing submission, Hayes argues that he and the other BitMEX executives began planning to implement a KYC program in May 2019, and asserts that this was "voluntar[y]" or

---

[7] The Government originally briefed the admissibility of this conduct as direct evidence of the charged crimes and as potential 404(b) material in its motion *in limine*, and the Court reserved decision. For purposes of sentencing, Hayes' lies to HSBC Hong Kong are appropriately considered both because they were intertwined with and an integral part of the crime of conviction and as part of his "background, character, and conduct." 18 U.S.C. § 3661.

Indeed, Hayes' sentencing submission provides further context to a question the Court raised during the conference on the motions. The Court reserved decision on whether this information would be admissible, but noted that "one of the underpinnings of the argument that the defendants were attempting to separate themselves from any association with Bitcoin, appears to strain credulity in view of the government's arguments about the prominence of the defendants in Bitcoin." As the defendant himself argues, however, "[i]n 2016 and the first half of 2017," namely when he and Delo began their scheme of lying to HSBC, his "business began to gain some limited traction, but growth was slow and revenues remained modest." Def. Mem. at 8. In other words, he was *not* particularly prominent in the crypto space when he lied to HSBC.

"proactive". Def. Mem. at 15. What he neglects to mention is that this was six months ***after*** the CFTC went overt in its investigation into BitMEX in November 2018, and after the CFTC had already served a subpoena on the company and deposed Reed, Dwyer, and other BitMEX employees, in which each was asked numerous questions about BitMEX's KYC program. At that point, the company knew that it was under regulatory scrutiny and was likely simply trying to forestall an enforcement action. What is notable is that, even though the company claimed that it was planning to implement a KYC program, it took essentially no steps toward actually doing so for over a year, only finally announcing that a KYC program was coming in August 2020. The actual program did not materialize until December 2020, after Hayes and his co-defendants had been indicted.

II. Procedural History

On October 1, 2020, Hayes' co-defendant Samuel Reed was arrested in Massachusetts, and the Indictment was unsealed. Hayes self-surrendered in Hawaii on April 6, 2021. After pre-trial motion practice, he ultimately entered a plea of guilty to Count One of the Indictment, violating the Bank Secrecy Act, in violation of Title 31, United States Code, Sections 5318 and 5322; and Title 31, Code of Federal Regulations, Sections 1026.210 and 1026.220, about a month before trial was scheduled. He is the first defendant to be sentenced in this case. His sentencing is scheduled for May 20, 2022.

III. Presentence Investigation Report

The Probation Office has calculated the offense level as follows, and as consistent with the plea agreement: (1) pursuant to U.S.S.G. § 2S1.3(a)(1), the base offense level is 8; (2) pursuant to U.S.S.G. §3B1.1(a), because the defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive, four levels are added; (3) two levels are removed for acceptance of responsibility, so the specific offense level is 10. (PSR ¶¶ 63–72). The defendant has no criminal history points, and is in Criminal History Category I.

This offense level and criminal history category lead to a Guidelines range of 6 to 12 months' imprisonment. (PSR ¶ 106.) The Government agrees with the Probation Office's calculation.

Probation has recommended a non-incarceratory sentence, with two years' probation. (PSR p. 40). This recommendation is based on Probation's apparent view that this crime is "a technical violation of banking law," and "that cryptocurrency and the regulations governing it, were and still are in its relatively early stages of development," including when the defendant and his co-conspirators launched BitMEX. (PSR p. 42). Probation also cites to the $10 million fine the defendant has agreed to pay.

IV. An Incarceratory Sentence Above the Stipulated Guidelines Range is Appropriate

A. Applicable Law

As the Court knows well, the Sentencing Guidelines are no longer mandatory after *United States v. Booker*, 543 U.S. 220 (2005). "[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007). After making the initial Guidelines calculation, a sentencing judge must consider the factors outlined in Title 18, United States Code, Section 3553(a), and "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing: "a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation." *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)).

In light of *Booker*, the Second Circuit has instructed that district courts should engage in a three-step sentencing procedure. *See Crosby*, 397 F.3d at 111-13. First, the Court must determine the applicable Sentencing Guidelines range, and in so doing, "the sentencing judge will be entitled to find all of the facts that the Guidelines make relevant to the determination of a Guidelines sentence and all of the facts relevant to the determination of a non-Guidelines sentence." *Id*. at 112; *see also United States v. Corsey,* 723 F.3d 366, 375 (2d Cir. 2013) ("Even in cases where courts depart or impose a non-Guidelines sentence, the Guidelines range sets an important benchmark against which to measure an appropriate sentence."). Second, the Court must consider whether a departure from that Guidelines range is appropriate. *See Crosby*, 397 F.3d at 112. Third, the Court must consider the Guidelines range, "along with all of the factors listed in section 3553(a)," and determine the sentence to impose. *Id.* In so doing, it is entirely proper for a judge to take into consideration his or her "own sense of what is a fair and just sentence under all the circumstances." *United States v. Jones*, 460 F.3d 191, 195 (2d Cir. 2006).

B. Discussion

A significant sentence of incarceration, above the applicable Sentencing Guidelines range of 6 to 12 months, is necessary to comply with the purposes set forth in 18 U.S.C. § 3553(a). Hayes' calculated and prolonged effort to violate the BSA on a large scale warrants a substantial period of incarceration. While any violation of the BSA undermines the nation's financial system, this case is unique in its extent and magnitude. The defendant's violation was not an isolated lapse in judgment or a temporary lapse in his operation of an otherwise law-abiding business. Rather, over the course of years, and as his company grew into one of the largest cryptocurrency trading platforms in the world, the defendant made a conscious and deliberate choice to operate the company in constant violation of the law. Moreover, Hayes earned enormous personal profits while operating BitMEX, and operated as its CEO and public face. He designed the company to allow its users to open accounts, transact, and move money, anonymously, without any KYC or AML controls. As the defendant knew, such a platform would be, and was, a magnet for criminals looking to launder the proceeds of their illegal activity and commit other crimes. Those serious

crimes, his disrespect for U.S. law, and the need to deter both the defendant himself and others in the cryptocurrency world, all favor a substantial period of incarceration above the Guidelines range.

The History and Characteristics of the Defendant

The defendant's sentencing submission makes clear that he was a sophisticated and successful businessman, with an excellent education and strong professional network. Unfortunately, despite those advantages, he chose to put his talent and sophistication to work to create a cryptocurrency platform that operated in daily violation of the law. The company's stratospheric rise was in part due to its refusal to comply with its legal obligations under the BSA. He was the CEO, the public face, the leader of BitMEX and the criminal activity. This was a crime driven by greed, not necessity.

The defendant has submitted a number of letters attesting to his positive personal qualities and expressing support. It is, of course, appropriate for the Court to take these letters into account in connection with sentencing. However, these attestations to the defendant's positive qualities do not distinguish him from the typical defendant in a white-collar case. As Judge Marrero observed in another case, this collection of letters

> falls into a pattern advanced by a subset of the white collar criminal. This category encompasses a select class: distinguished, reputable, highly esteemed model citizens such as this defendant. The list of their achievements and virtues is long and impressive. Let us count the ways. At home, they are good family men and women, caring spouses, loving parents, loyal and reliable to friends. At work, they are looked up to as outstanding professionals and business partners. To their community's charities and public causes they are generous patrons and sponsors.

United States v. Regensberg, 635 F. Supp. 2d 306, 308 (S.D.N.Y. 2009), *aff'd*, 381 F. App'x 60 (2d Cir. 2010); *see also United States v. McClatchey*, 316 F.3d 1122, 1135 (10th Cir. 2003) ("excellent character references are not out of the ordinary for an executive who commits white-collar crime; one would be surprised to see a person rise to an elevated position in business if people did not think highly of him or her"); *United States v. Vrdolyak*, 593 F.3d 676, 682-83 (7th Cir. 2010) ("[I]t is usual and ordinary, in the prosecution of similar white-collar crimes . . . to find that a defendant was involved as a leader in community charities, civic organizations, and church efforts," and the defendant "should not be allowed to treat charity as a get-out-of-jail card" (citation and internal quotation marks omitted)).

The Government does not question that Hayes is a talented, accomplished, and influential person who has helped many others in his career. But these positive qualities, while admirable, do not set Hayes apart from other similarly situated white-collar defendants—individuals who are high-achieving and successful, but nonetheless chose to break the law for personal advantage.

The Government also notes that one of the attributes highlighted in the defendant's sentencing submission and supporting letters is his outspokenness and prominence in the world of cryptocurrency, which he refers to as his "cryptocurrency thought leadership." Unfortunately, this

case shows that the defendant chose to use his influence to promote a vision for the crypto industry that was in direct contradiction to the law, and calculated to undermine government regulations. As noted above, the defendant routinely criticized and mocked KYC requirements, and made it clear that he had no interest in complying with them. Moreover, the defendant even criticized other cryptocurrency industry participants who did require KYC, and argued that these requirements were not desired by crypto users because they might prevent them from engaging in illegal activity. For instance, in 2019, when Facebook announced a plan for a cryptocurrency called Libra, Hayes wrote a mocking blog post warning that "you can bet that converting assets into Libra will encounter KYC. And let's be clear, any request from a government agency to freeze a transaction will be met with compliance. Therefore, do not use Libra to buy your mood-altering substance(s) of choice."[8] Thus, while it may be true that the defendant is a "thought leader" in cryptocurrency, he deliberately used that leadership role to undermine regulations and promote the idea that crypto should be an anonymous asset free from law enforcement oversight.[9]

The defendant also highlights his "philanthropic and community service." However commendable they may be, these acts are unexceptional and insufficient to warrant a below-Guidelines sentence. *See* U.S.S.G. § 5H1.11 ("Civic, charitable, or public service; employment-related contributions; and similar prior good works are not ordinarily relevant in determining whether a departure is warranted."). Additionally, the fact that the defendant was able to give several million dollars to charity no doubt resulted in large part from the fact that he personally received some $150 million in dividends from BitMEX while the company systematically flouted the BSA for a period of five years.

The Seriousness of the Offense

A substantial sentence is needed because the defendant was a leader of a serious criminal enterprise. The BSA is designed to safeguard the financial system, both in the United States and around the world, from illicit use, and to combat money laundering. Financial institutions are required to implement AML programs so that the institutions do not foster criminal activity or lead to the diversion of victim funds. Cryptocurrency compounds the need for such programs because of the technology's pseudonymity; without KYC and AML, a user of cryptocurrency could evade law enforcement by hiding behind the string of numbers describing their wallet address.

By operating BitMEX without an AML program, Hayes created a significant platform for cryptocurrency users to do exactly that. Due to Hayes' criminal conduct, the full scope of the illegal behavior that BitMEX enabled cannot be precisely estimated. It is noteworthy, however, that FinCEN identified $200 million in suspicious transactions, a staggering sum. Similarly, Hayes' decisions, and his refusal to implement a full KYC and AML program, meant that it was

---

[8] *See* https://blog.bitmex.com/libra-zuck-me-gently/ (accessed May 12, 2022).

[9] This commentary went far beyond mere "libertarian viewpoints" critical of the Government, Def. Mem. at 18 n.13, particularly in light of his self-described role as a leader in the cryptocurrency industry, insofar as it fostered the view that cryptocurrency companies should evade the BSA to become as successful as BitMEX.

more likely that BitMEX would allow sanctioned parties to trade, which they did. That sanctions evasion carries substantial costs to the U.S. financial system and U.S. national security interests.

Nor was Hayes somehow unaware that he was creating a risk that his platform could be used for unchecked money laundering. As he acknowledges, he knew for years that he was required to have KYC and AML programs but willfully permitted users to transact anonymously with no controls, and did so despite repeated warnings from law enforcement around the world about suspicious activities on the platform. His failure to implement an AML program meant that it was harder for law enforcement to identify criminal activity and track victim funds. This was no mere regulatory mistake. Hayes refused to implement an AML program knowingly and intentionally.

An above-Guidelines sentence is also appropriate given Hayes' frequent lies about BitMEX's operation. Hayes could only maintain the fiction that BitMEX need not comply with the BSA through his repeated lies about its U.S. operations and U.S. customers. Hayes also lied to HSBC, in a way that underscores his criminal culpability in this case. The Government understands that the bank would have performed more due diligence and possibly even restricted the account-holder's ability to make U.S. dollar wire transfers if it had known the truth, that Shine Effort was acting on behalf of an unregulated cryptocurrency exchange that performed no AML program. Those lies led HSBC to allow over a hundred million dollars flow through the account, despite the substantial regulatory and reputational risk to the bank.[10]

The Need to Promote Respect for the Law

The need to promote respect for the law is also a critical factor here. This crime was a willful violation of U.S. law, undertaken for years, purely for the defendant's financial advantage. He attempts to justify his conduct by explaining that he initially decided it was "not practicable" to follow the law because BitMEX was at its inception "thinly-resourced." Def. Mem. at 11 n.6. But he himself cites to a chart showing explosive monthly revenue exceeding $10 million soon after October 1, 2017. Def. Mem. at 8–9.[11] That means that Hayes had more than enough resources to follow the law. He used his wealth to retain some of the most sophisticated attorneys in this country to assist BitMEX, and indeed was able to arrange a direct meeting with the CFTC, where he could discuss BitMEX's platform and attempt to follow any guidance given.[12] His decision not

---

[10] In a somewhat similar recent case, Judge Rakoff imposed incarceratory sentences of 18 and 36 months' for defendants who had deceived banks in order to transfer more than a hundred million dollars through their accounts, even though the banks suffered no loss. *United States v. Weigand and Akhavan*, 20 Cr. 188 (S.D.N.Y.).

[11] Later data showed that the Company had revenues exceeding $20 million a month by January 1, 2018.

[12] Hayes' assertion that he showed "prescien[ce]" that the CFTC would not approve BitMEX's business model because of its features is aggravating, not mitigating. Def. Mem. 11 n.6. If the defendant knew that BitMEX could only succeed by violating the law then he should not have founded BitMEX, and either identified a law-abiding enterprise that could succeed, or continued

to expend money on compliance emphasizes his criminal culpability. This is all the more so in light of Hayes' public expressions of disdain for KYC and AML regulations, and his general encouragement of others in the crypto sphere to ignore them.

Hayes' dismissive attitude toward the regulations intended to protect retail investors—and indeed his lack of concern for those investors—is illustrative of his general lack of respect for the law. Whether cryptocurrency companies agree with the law or not, the CEA is designed to protect retail investors. Hayes instead jokingly referred to his client base, oftentimes just regular people, as "degenerate gamblers," ignoring the material consequences his decisions had on individuals less sophisticated than an honors Wharton graduate with years in financial services.

Specific and General Deterrence

The need for general and specific deterrence weighs heavily in favor of a substantial, above-Guidelines sentence. The cryptocurrency industry is still an evolving market space, and new trading platforms are emerging seemingly by the day. It is a critical policy of the United States to ensure that these platforms comply with regulations such as the BSA, to prevent this new space from becoming an unregulated market where criminals can transact with impunity. *See, e.g.*, FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," *available at* https://www.fincen.gov/sites/default/files/shared/AML_CFT_Priorities(June%2030%2C%202021).pdf ("FinCEN notes that, while a substantial financial innovation, convertible virtual currencies (CVCs) also have grown as the currency of preference in a wide variety of online illicit activity."). One of the tools to encourage that is the deterrent effect of criminal prosecutions for willful violations, which depends in large part on meaningful sentences being imposed when the law is violated. The non-incarceratory sentence that the defendant requests would undermine that goal, and fail to deter either this defendant or other similarly situated defendants from committing similar crimes in the future.

The defendant's own sentencing submission makes it clear that there is a need for specific deterrence in this case. The defendant makes no secret of his intention to continue to operate in the cryptocurrency industry. Given his lengthy history of anti-regulatory and anti-law enforcement rhetoric and conduct in relation to cryptocurrency trading, there is an acute risk that he will return to criminal conduct if he does not perceive that there is a real cost to such criminal behavior. The defendant has paid a significant financial penalty, but it is only a small portion of the money he has made from operating BitMEX, and could easily be viewed as just a "cost of doing business" outside the law.[13] *SEC v. Rajaratnam*, 918 F.3d 36, 45 (2d Cir. 2019). A substantial sentence of

---

in his highly compensated jobs in finance. Of course it was easier to make money violating the law than it was to follow the law, but that is no justification to ignore the law.

[13] That argument is highlighted by Hayes' absurd suggestion that the Court should also factor in the "diminution in the value of BitMEX," Def. Mem. at 18, or the "tens of millions of dollars that BitMEX has spent in connection with remediation, compliance undertakings." Def. Mem. at 28 n.15. The Company has lost value because of his own crimes and regulatory violations. The compliance costs *should have been paid* from BitMEX's launch. Discounting his criminal sentence based on such a factor would be rewarding him for his criminal conduct.

incarceration is needed to send the message that such criminal conduct will carry consequences. The need for deterrence is especially acute where, as here, a crime has proven to be lucrative and has required great effort to detect and prosecute. "Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it." *United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018) (quoting *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994)).

Moreover, a substantial sentence is needed to foster general deterrence. There is no question that this case has been extremely closely watched in the cryptocurrency industry. BitMEX is a major player in that industry, and Hayes in particular has been a high-profile leader in crypto for years. The decision about whether to comply with the BSA is a calculated one that many other actors in the cryptocurrency space are making, which greatly raises the importance of general deterrence as a sentencing factor in this case. *See United States v. Peppel*, 707 F.3d 627, 637 (6th Cir. 2013) ("Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." (quotation marks omitted)). Compliance by cryptocurrency platforms will be unattainable if their operators believe there are no meaningful repercussions for failing to comply with the law, even if they are actually detected and successfully prosecuted.

The Guidelines Range and Other Defendants With Similar Conduct

An above-Guidelines sentence is also appropriate because the applicable Sentencing Guidelines are highly anomalous. Unlike many similar offenses, the Guidelines for this offense do not vary in accordance with the magnitude of the offense. While the defendant did receive leadership points for his role in the offense, his Guidelines Range is otherwise the same as it would be if he had run a small check-cashing storefront that had a real but willfully inadequate AML program. Clearly his culpability is substantially greater than such an offense, as he operated a massive offshore financial marketplace that openly proclaimed its lack of any AML program. The Court should consider the scope of the defendant's criminal conduct, the trillions of dollars which BitMEX allowed to trade, the hundreds of millions of dollars the defendant earned, and conclude that the Sentencing Guidelines are too low for such an offense. *Cf. United States v. Tokhtakhounov*, 607 F. App'x 8, 12 (2d Cir. 2015) (affirming above-Guidelines sentence in case involving laundering of gambling proceeds where district court found the guidelines understated the seriousness of the conduct because the "gambling Guidelines do not consider the amount of money gambled in calculating the base offense level.")

A sentence above the Guidelines Range would also comport with the sentences imposed in the most closely analogous cases, where the defendants were executives at cryptocurrency companies which circumvented AML restrictions by operating unlicensed money transmitting businesses, in violation of 18 U.S.C. § 1960. In several recent such cases, courts have imposed sentences in an average range that is higher than the Guidelines Range here. *See, e.g., United States v. Shrem*, 14 Cr. 243 (S.D.N.Y.) (JSR) (two year sentence for defendant, who was the CEO and compliance officer of a Bitcoin exchange company that operated as an unlicensed money services business and who deliberately allowed a specific customer to circumvent AML restrictions); *United States v. Marmilev*, 13 Cr. 368 (S.D.N.Y.) (DLC) (five year sentence for defendant who

was Chief Technology Officer at unlicensed money transmitting business in digital currency, some of which he knew were derived from criminal activity); *United States v. Chukharev*, 13 Cr. 368 (S.D.N.Y.) (DLC) (three year sentence for minor participant at the same unlicensed money transmitting business in digital currency as Marmilev, but who did not know about its use for criminal activity); *United States v. Tetley*, 17 Cr. 738 (C.D. Cal.) (sentence of a year and a day for a defendant who operated an unlicensed money services business in cryptocurrency, as well as commit money laundering through that business); *United States v. Lord*, et al., 15 Cr. 240 (W.D. La.) (46 months' sentence for operating an unlicensed money services business in cryptocurrency). If anything, given the size and scope of the defendant's operation, his culpability exceeds that of the defendants in these analogous cases.[14] It would be a significant deviation to impose a non-incarceratory sentence in this case as the defendant requests, and even a within-Guidelines sentence would be lower than is necessary to comply with the purposes set forth in 18 U.S.C. § 3553(a).

Nor does the fact that this is supposedly a "first-of-its-kind prosecution" militate in favor of the defendant's requested sentence. Def. Mem. at 25. That argument did not convince the judges who imposed lengthy sentences on the operators of the crypto unlicensed money transmitting businesses in the cases listed above, many of whom were the first (or near the first) such defendants prosecuted.

Probation's Recommendation is Inadequate

Probation has recommended a non-incarceratory sentence, reasoning that this was a technical violation of banking law, that the regulatory environment for cryptocurrency was in early stages, and that the fine sum is sufficient to disgorge the ill-gotten gains from the offense. (PSR p. 42). Each reason is mistaken.

This was no technical violation of the law. The BSA's AML and KYC requirements are not obscure technicalities: they underpin and are designed to protect the global financial system. Nor is this a case in which there was some technical noncompliance with the BSA; on the contrary, BitMEX made no attempt to comply with the law and did not have an AML or KYC program at all. Moreover, this case is a criminal matter not because Hayes accidentally violated a technicality, but because he did so willfully.

Nor was the regulatory environment unclear. As the defendant agrees, he was entirely aware of the regulatory environment and its import for BitMEX. Hayes has admitted that he understood in September 2015 that "BitMEX could be subject to CFTC jurisdiction, including a requirement to conduct KYC, if the company served U.S. customers." Def. Mem. at 11.

---

[14] Unlike the Guidelines at issue here, the Guidelines for Section 1960 *do* refer to the 2B1.1 table and therefore vary with the magnitude of the offense. U.S.S.G. § 2S1.3(a)(2); U.S.S.G. § 2S1.1(a)(2). But violating the BSA in the manner the defendant did shows more disrespect for the law than operating an unlicensed MSB: the defendant could only be convicted because he violated the law willfully, whereas Section 1960 does not require proof of awareness "of the obligation to register a money-transmitting business." *United States v. Mazza-Alaluf*, 607 F. Supp. 2d 484, 489 (S.D.N.Y. 2009), *aff'd*, 621 F.3d 205 (2d Cir. 2010).

Finally, the $10 million fine is not a sufficient punishment under Section 3553(a). That sum is a reasonable if conservative approximation of the direct pecuniary gain he derived from the offense. But that does not capture the unquantifiable indirect value, since the lack of an AML program allowed BitMEX to grow its lucrative business, given its prominent place in the company's marketing efforts. Even assuming that the fine amount were the only benefits the defendant received from the violation, that does nothing more than disgorge ill-gotten gains; it is not a punishment for his criminal conduct. Such a sentence would have a negligible deterrent effect on the operators of other cryptocurrency companies, who could simply violate the law Hayes did, try to evade law enforcement detection, but even if caught, pay nothing more than those wrongful profits they derived as a direct result of the offense.[15]

Thus, each premise of Probation's recommendation is wrong, and do not support the proposed sentence.

V. Conclusion

For the reasons stated above, the Court should impose a significant sentence of incarceration, above the applicable Sentencing Guidelines range of 6 to 12 months, which is necessary to comply with the purposes set forth in 18 U.S.C. § 3553(a).

Very truly yours,

DAMIAN WILLIAMS
United States Attorney

by: Samuel Raymond
Samuel L. Raymond
Thane Rehn
Jessica Greenwood
Assistant United States Attorneys
(212) 637-6519

cc: Counsel for Defendant Arthur Hayes

[15] Additionally, because violations of the Bank Secrecy Act do not carry forfeiture, the fine is not a separate punishment after the defendant forfeits his criminal proceeds; instead, the fine in this case only serves the basic disgorgement function.